Deloitte.

Riscos Cibernéticos e Segurança da Informação na América Latina e Caribe

Tendências 2019

Março de 2019

Cyber

A evolução da gestão da segurança da informação

A Deloitte tem o prazer de apresentar os resultados do estudo **"Tendências em Gestão de Riscos Cibernéticos e Segurança da Informação na América Latina e Caribe 2019"**

As organizações na América Latina e Caribe (AL&C) estão inseridas em um cenário de forte desenvolvimento de negócios digitais e de maior exposição às ameaças cibernéticas inerentes a esse novo contexto.

O caminho para se adaptar aos riscos cibernéticos atuais deve começar a ser trilhado a partir da tomada de consciência e da conscientização dos níveis executivos da organização sobre as ameaças do novo ambiente digital de negócios.

Convidamos o leitor a consultar o presente documento, que contém um resumo das principais tendências de riscos cibernéticos e segurança da informação, além da descrição dos aspectos-chave identificados a partir das respostas recebidas das organizações participantes.

Julio Laurino
Sócio-líder da prática de Cyber Risk
Deloitte Brasil

Andrés L. Gil
Sócio-líder da prática de Cyber Risk para Américas

Índice

Introdução

Informações gerais sobre a pesquisa

Escopo e extensão

A pesquisa teve como objetivo identificar as tendências da gestão de riscos cibernéticos e segurança da informação na América Latina

O estudo focou a análise das tendências surgidas a partir da transformação e digitalização dos negócios

150 **Organizações participantes**

12 **Países**

7 **Indústrias / setores**

Informações gerais sobre a pesquisa

Países e indústrias participantes

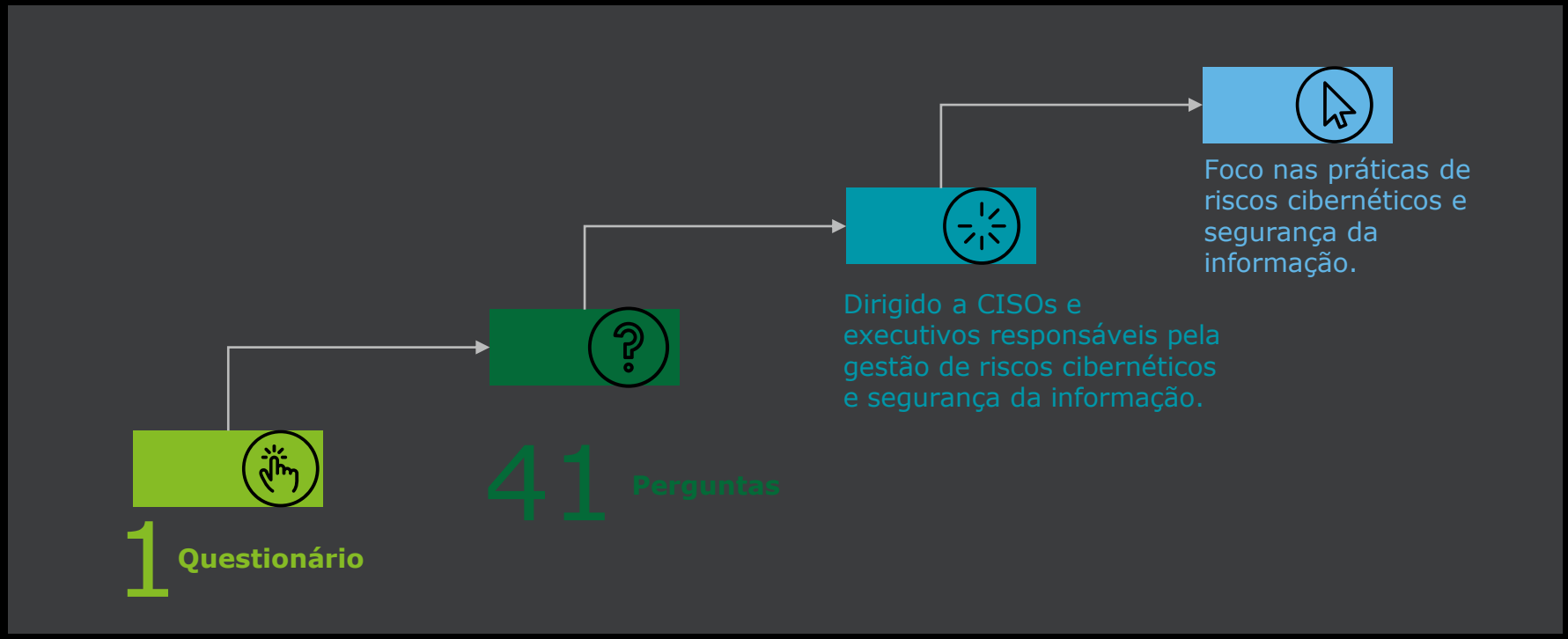
Serviços financeiros	44.7%
Manufatura	10.7%
Tecnologia, Mídia e Telecomunicações	10.6%
Serviços	10%
Petróleo, Gás e Mineração	10%
Outros	8%
Setor Público	6%

Informações gerais sobre a pesquisa

Perfil dos entrevistados

Informações gerais sobre a pesquisa

Processo de compilação das informações



D Indica a perspectiva da Deloitte

Período de campo

Julho de 2018 — **Outubro de 2018**

Principais tendências identificadas

Principais tendências identificadas

4 de cada 10 organizações sofreram um **incidente de segurança cibernética** nos últimos 24 meses.

70% das organizações afirmam não ter certeza da eficácia de seu processo de resposta diante de desses incidentes, enquanto **apenas 3% realizam simulações** para testar suas capacidades efetivas de resposta diante de um evento cibernético.

D

Seguindo a tendência observada em anos anteriores, e apesar do aumento dos investimentos em segurança da informação, as organizações continuam sofrendo falhas de segurança.

Nesse contexto, é imperativo que os investimentos sejam destinados não somente à implantação de medidas de proteção, mas também à melhoria das capacidades de monitoramento e resposta, aspecto que continua como uma pendência significativa das organizações na AL&C.

As organizações da América Latina estão **aumentando seus orçamentos** dedicados à gestão de riscos cibernéticos e à segurança da informação.

89% dos entrevistados atribuem uma **importância muito alta à gestão de riscos cibernéticos** em um contexto de negócios cada vez mais digital.

D

A problemática de riscos cibernéticos e segurança da informação continua crescendo, o que requer orçamentos mais altos nessa área.

De acordo com a visão dos executivos entrevistados, suas organizações consideram que essa é uma área chave no cenário atual de digitalização dos negócios e de ameaças emergentes.

Principais tendências identificadas

As organizações possuem **capacidades limitadas** de monitoramento de segurança cibernética e inteligência de ameaças.

Apenas 31% das empresas colocam em prática medidas de inteligência para detectar riscos e compartilham ameaças com outras organizações.

D

As organizações na AL&C estão em um estágio inicial no que se refere às capacidades de inteligência de ameaças, com processos básicos de monitoramento.

Para poder se preparar e responder rapidamente diante dos novos ataques cibernéticos, é preciso que as habilidades das empresas reflitam não apenas sobre o que acontece da porta para dentro, mas também entendam em profundidade as ameaças que afetam as organizações em geral – e seu setor de atuação em especial – obtendo informações de inteligência que sejam relevantes.

7 de cada 10 organizações **implantaram um programa de conscientização** sobre segurança cibernética.

D

Percebe-se a importância de capacitar e conscientizar seus colaboradores sobre riscos cibernéticos e o seu impacto para a organização.

O tempo do executivo de riscos cibernéticos e segurança da informação deve ser em boa parte dedicado a seus pares, à alta administração e aos acionistas sobre essa problemática, para obter a visibilidade adequada e apoio na execução de programas que permeiem toda a empresa.

Principais tendências identificadas

Evolução da gestão de riscos cibernéticos e segurança da informação

D

A área de **gestão de riscos cibernéticos e segurança da informação** está evoluindo para atingir um novo paradigma que inclui quatro componentes centrais e estratégicos:

Governança

Estabelece a visão, a estratégia, a função e as responsabilidades da área de gestão de riscos cibernéticos e segurança da informação – levando em conta os imperativos do negócio, as leis, as regulações, além dos recursos humanos e tecnológicos.

Segurança

Tem como foco a proteção da informação e aplicação das tecnologias que dão suporte aos processos-chave do negócio, implantando controles adequados para as vulnerabilidades às quais a organização está sujeita.

Vigilância

Busca o estabelecimento de uma cultura que permeie toda a organização para que cada profissional fique atento às ameaças. Desenvolve também padrões de comportamento que possam prever uma ofensiva à informação.

Resiliência

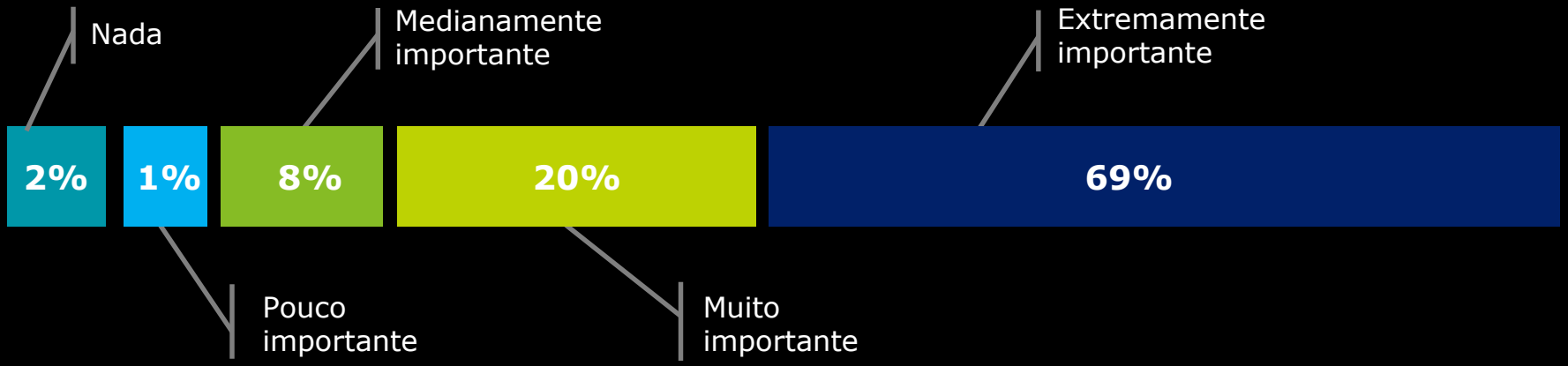
Significa ter a capacidade de controlar rapidamente o dano em caso de incidentes e mobilizar os recursos necessários para minimizar o impacto – incluindo custos diretos e paralisação do negócio, além de danos à reputação e à marca.

Resultados

Governança

Estratégia e estrutura de gestão

Importância da segurança cibernética para as organizações



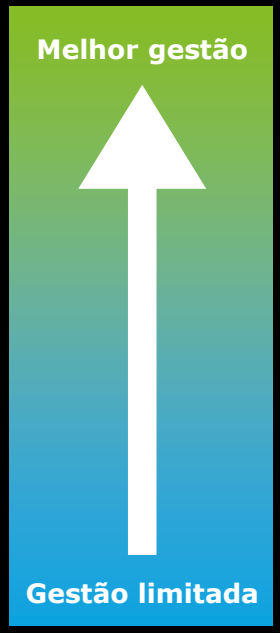
D

Para as organizações na AL&C, a segurança cibernética é um componente bastante importante do seu modelo de governança e gestão.

No entanto, podem existir inconsistências entre a manifestação dessa importância versus os orçamentos alocados e/ou o nível de maturidade de suas práticas de gestão de segurança cibernética.

Governança de segurança cibernética

Definição de funções e responsabilidades



Governança de riscos cibernéticos e segurança da informação formalizadas e em funcionamento	13%
Funções e responsabilidades definidas, claras, destinadas à detecção, prevenção e proatividade	7%
Funções e responsabilidades definidas e claras	12%
Funções e responsabilidades definidas	37%
Não exigem funções específicas para administrar a segurança cibernética	31%

D

Uma área de segurança cibernética melhor e mais especializada garantirá que as organizações tomem decisões mais eficazes, com uma visão precisa de futuro e com capacidades para facilitar o desenvolvimento de negócios digitais de forma segura.

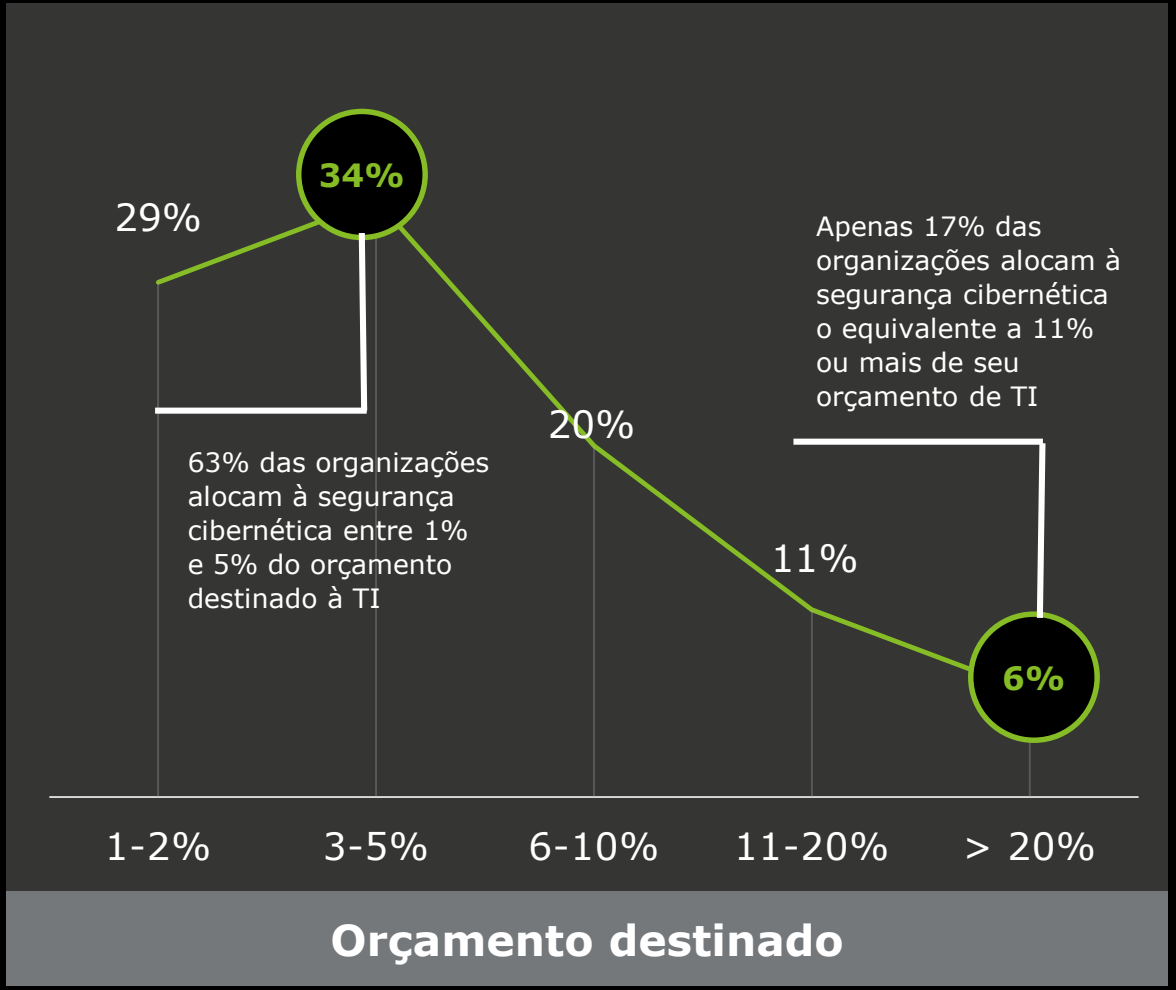
A formalização de uma estrutura de governança de segurança cibernética é um passo importante para fortalecer as competências e a maturidade da organização nessa área.

Orçamento dedicado à segurança cibernética

D

Possuir um orçamento próprio é fundamental para o crescimento e a maturidade da área de riscos cibernéticos e segurança da informação.

O orçamento deve estar alinhado com o nível de aceitação de risco por parte da organização.



Gestão de segurança cibernética integrada com outros processos-chave

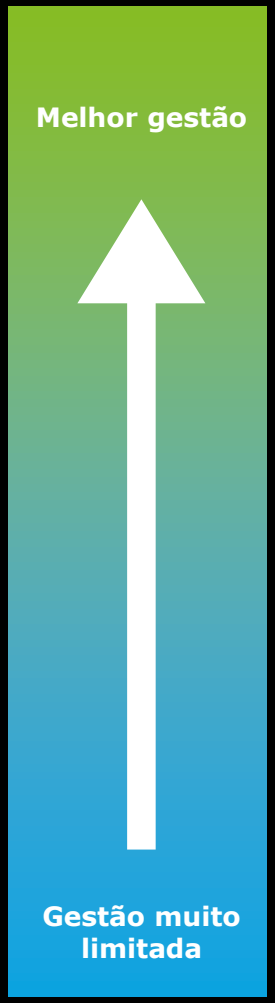
As mudanças nas configurações resultam em atualizações automáticas no programa de gestão de vulnerabilidades

Existe certa comunicação entre a área de segurança e a gestão de riscos

Existem métricas de riscos cibernéticos em algumas unidades de negócio específicas

Indicadores-chave de riscos cibernéticos estão definidos e são monitorados

Não há atividades específicas



D

As organizações na AL&C encontram-se em um processo de integração de suas operações de segurança cibernética com outros processos de gestão.

É importante desenvolver e monitorar indicadores de riscos cibernéticos, a fim de ter um entendimento adequado do nível de exposição e maturidade da organização em suas práticas de segurança cibernética.

Utilização de serviços administrados e terceirização como estratégia para complementar capacidades cibernéticas

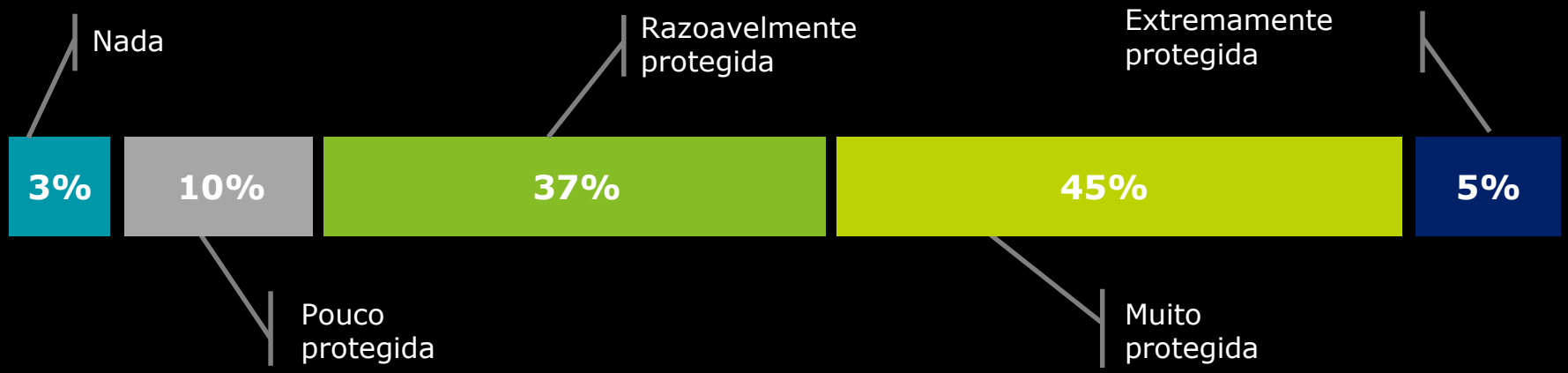
D

As dificuldades que as organizações da AL&C enfrentam em relação à disponibilidade de recursos humanos qualificados – tanto em termos de quantidade como em qualidade – somadas à complexidade da gestão, levaram um grande número de organizações a terceirizarem processos de segurança cibernética.

Definir uma estratégia de uso de fornecedores especialistas para dar suporte à gestão cibernética é um aspecto-chave do modelo de governança de segurança cibernética no contexto atual.

Segurança
Proteção da informação

Nível de proteção cibernética das organizações



D

A metade das organizações estima-se muito protegida em relação aos riscos cibernéticos. No entanto, a maturidade de certas práticas-chave na gestão dessas ameaças, como monitoramento, resposta a incidentes e inteligência cibernética, pode indicar um grau de otimismo maior do que a real capacidade dessas práticas.

As empresas devem considerar que a digitalização de seus negócios e o incremento da sofisticação dos ataques requerem o desenvolvimento de novas habilidades.

Práticas para prevenir o roubo de informações

A tecnologia de DLP implantada é continuamente refinada

15%

Políticas de proteção de dados foram desenvolvidas no âmbito de cada divisão/departamento e são constantemente revisadas e melhoradas

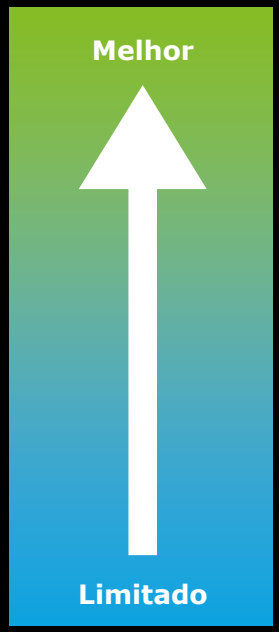
9%

Políticas de proteção de dados foram desenvolvidas de maneira básica, incluindo alarmes e algum nível de monitoramento

47%

A política de proteção de dados não foi implantada

29%

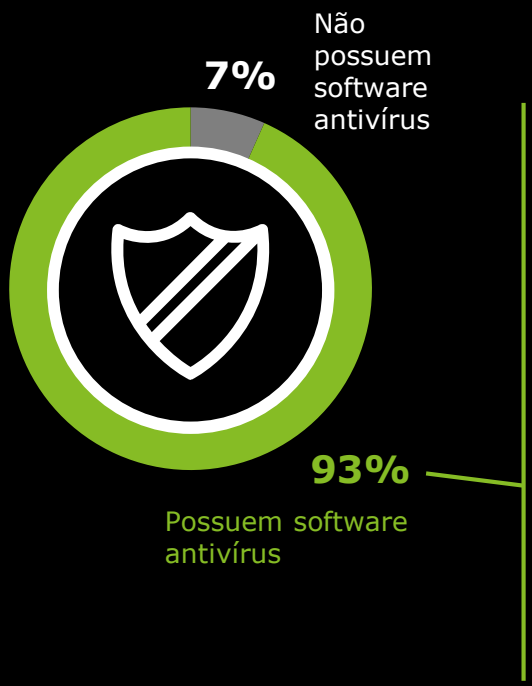


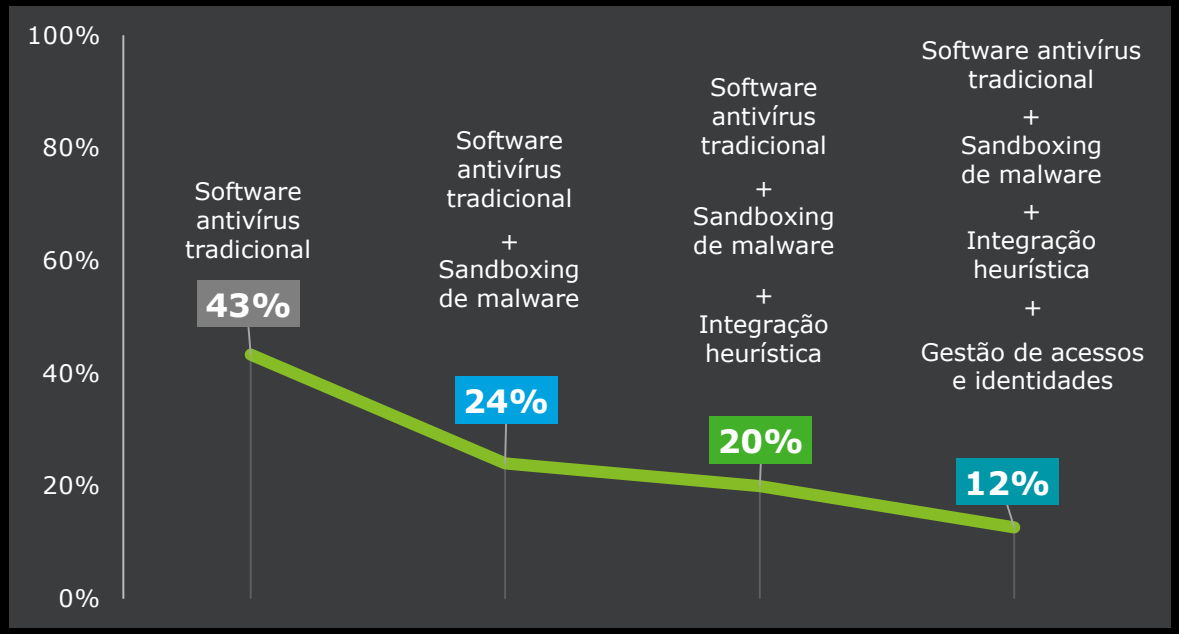
D

As informações de uma organização são, hoje, um de seus ativos mais importantes.

De modo geral, as organizações na AL&C encontram-se em um estágio médio de proteção de seus dados, com a necessidade de focar e investir em tecnologias que dêem suporte às políticas definidas.

Capacidades tecnológicas de detecção e proteção frente a ameaças de malware / código malicioso



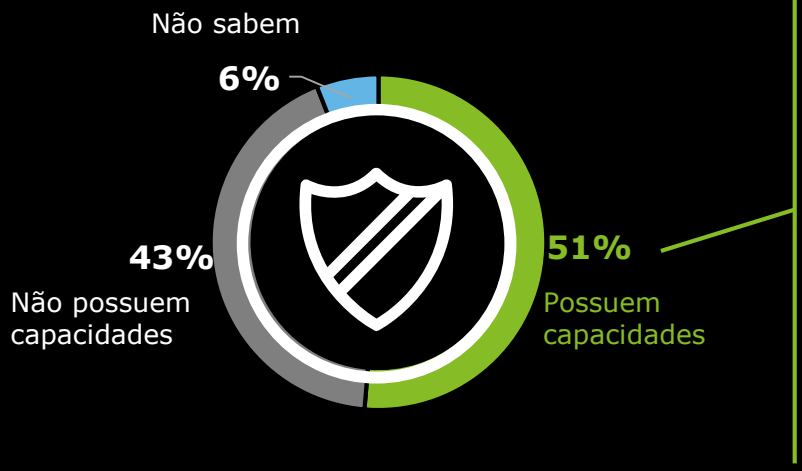


D

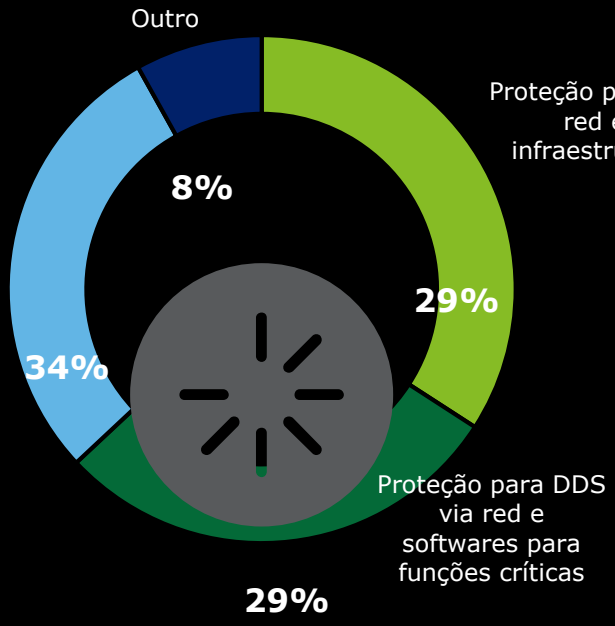
No contexto atual de ameaças cibernéticas, as organizações devem contar com diferentes tecnologias destinadas a proteger suas informações e seus sistemas contra malwares ou códigos maliciosos.

Apesar de observar-se na AL&C o uso de tecnologias adicionais ao tradicional antivírus, ainda existem oportunidades de melhoria nessa área de proteção crítica.

Proteção contra ataques de recusa de serviço



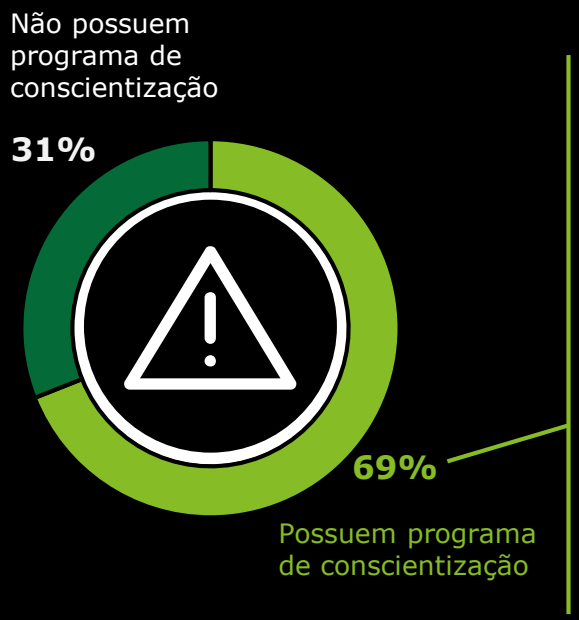
Ferramentas para DDS testadas periodicamente para garantir a eficácia

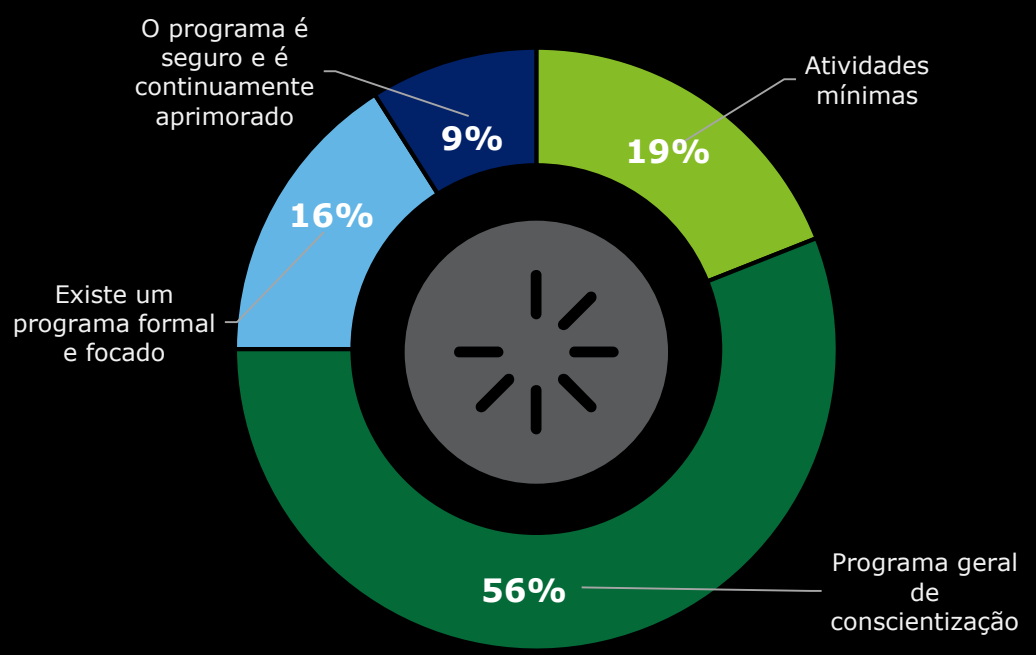


D

A importância dos ataques de recusa de serviço continua a crescer nas operações das empresas, ocasionando fortes impactos. As organizações devem trabalhar de forma sistêmica na otimização e atualização de ferramentas para a proteção de DDoS, que permitam diminuir os riscos desses incidentes.

Programa de conscientização sobre ameaças cibernéticas





D

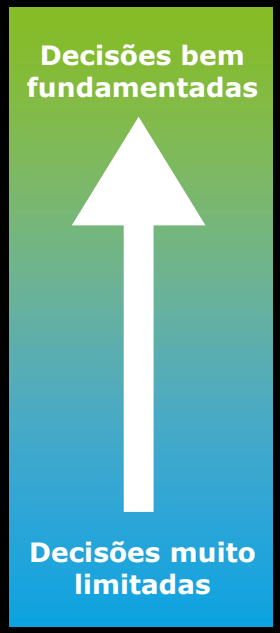
O fator humano ainda é imprescindível para a segurança da informação. Sua importância reside no fato de que ele é uma porte de entrada nas organizações por meio da qual muitos controles tecnológicos podem ser burlados.

A conscientização sobre a importância de sua função e seu compromisso com a informação continuam a ser a melhor medida para evitar vulnerabilidades.

Vigilância

Monitoramento proativo de ameaças e eventos

Análise de informações de eventos e ameaças de segurança cibernética

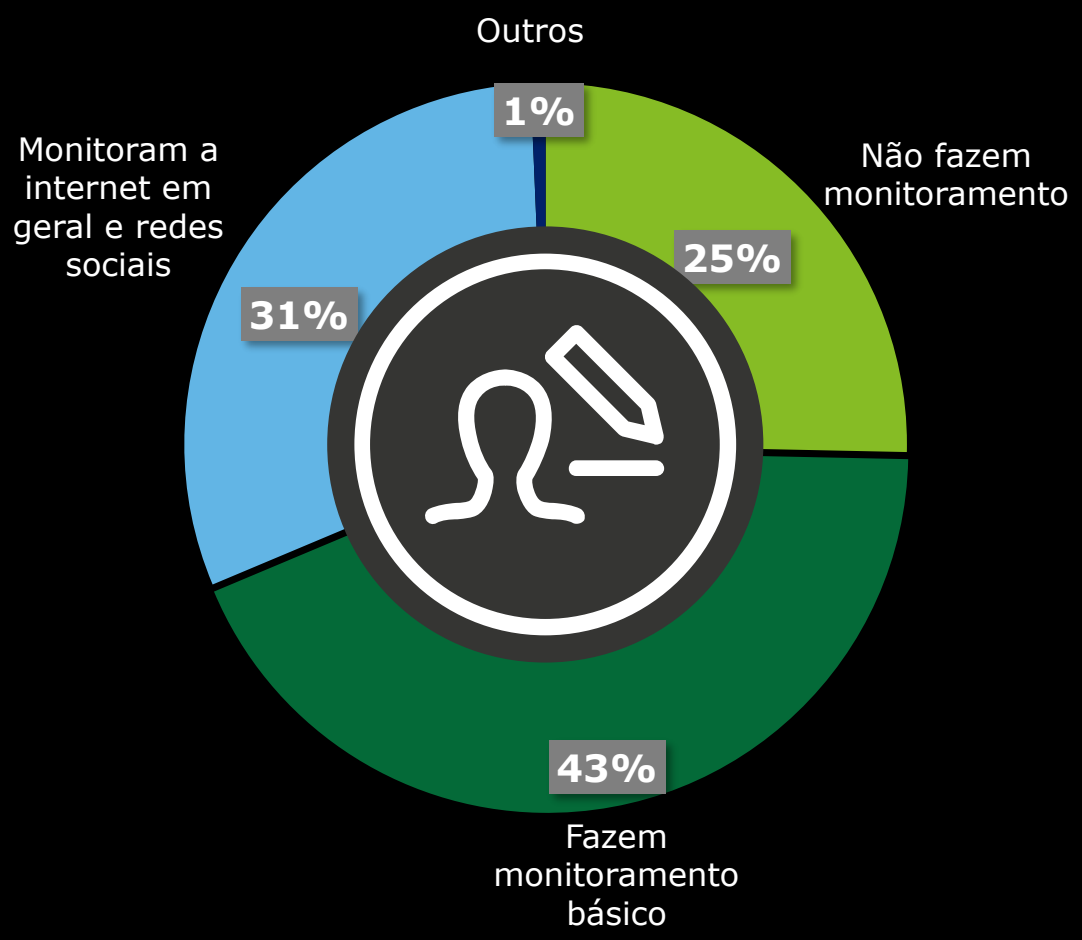


Análise de eventos com base em casos de uso de negócio para suporte de decisões em tempo real	28%
Análise de comportamento de usuários (UBA) e análise de tráfego	23%
São analisadas informações de infraestrutura, rede e perfil de sistemas	42%
As informações não são analisadas	7%

D

As empresas da AL&C devem otimizar seus processos para compilar registros, analisar tendências e anomalias; e utilizar os resultados para tomar decisões mais precisas.

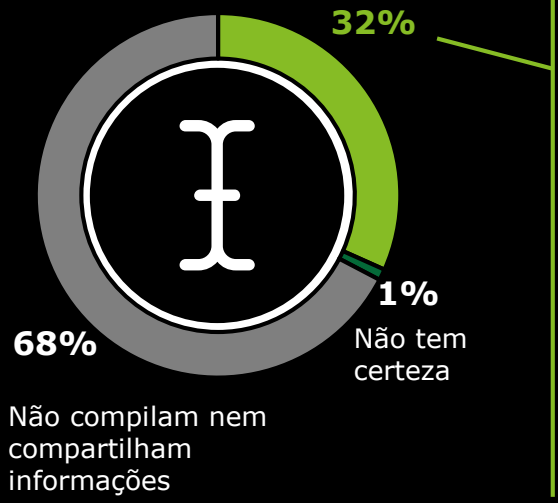
Monitoramento de informações disponíveis na internet

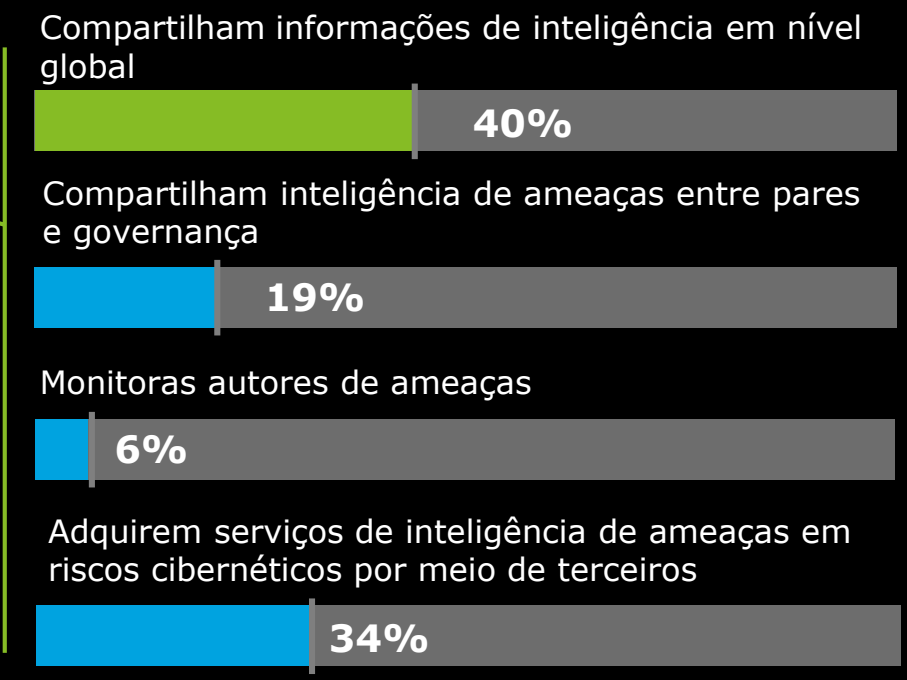


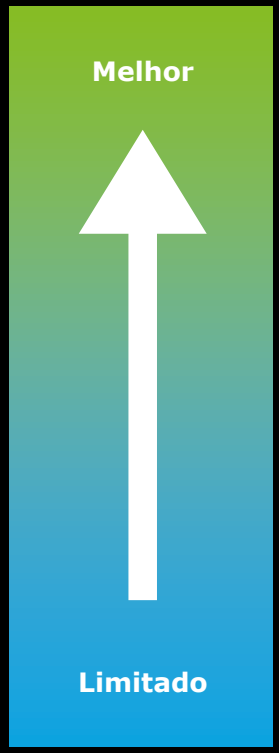
D

A proliferação de informações na internet, e sua capacidade de impactar a reputação da organização, demanda que as fontes públicas de informações sejam monitoradas de forma proativa, para descobrir informações sensíveis e aplicar ações corretivas o mais rápido possível

Inteligência de ameaças







D

Em um ambiente de constantes mudanças tecnológicas, em que o modelo de operação costuma ser 24/7, possuir informações atualizadas sobre a situação de ameaças e riscos cibernéticos é uma competência-chave a ser desenvolvida pelas organizações.

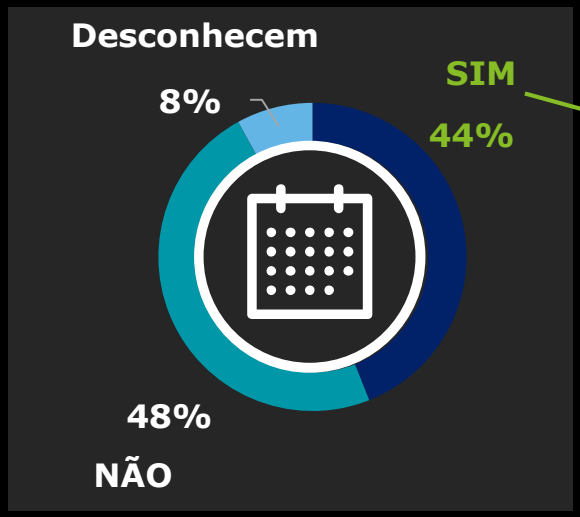
Na AL&C ainda há muito trabalho a ser feito para coletar, armazenar e compartilhar informações para uma inteligência que coloque em prática processos internos de preparação e respostas.

Resiliência

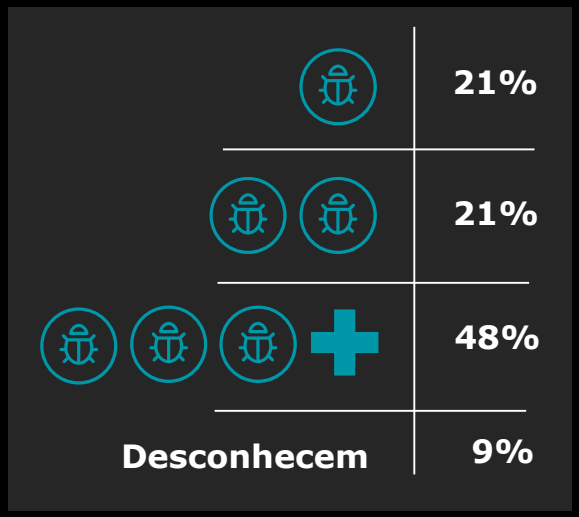
Resposta rápida e eficaz

Incidentes de segurança cibernética sofridos pelas organizações

Sofreram ataques cibernéticos nos últimos 24 meses



Quantidade de ataques cibernéticos sofridos nos últimos 24 meses

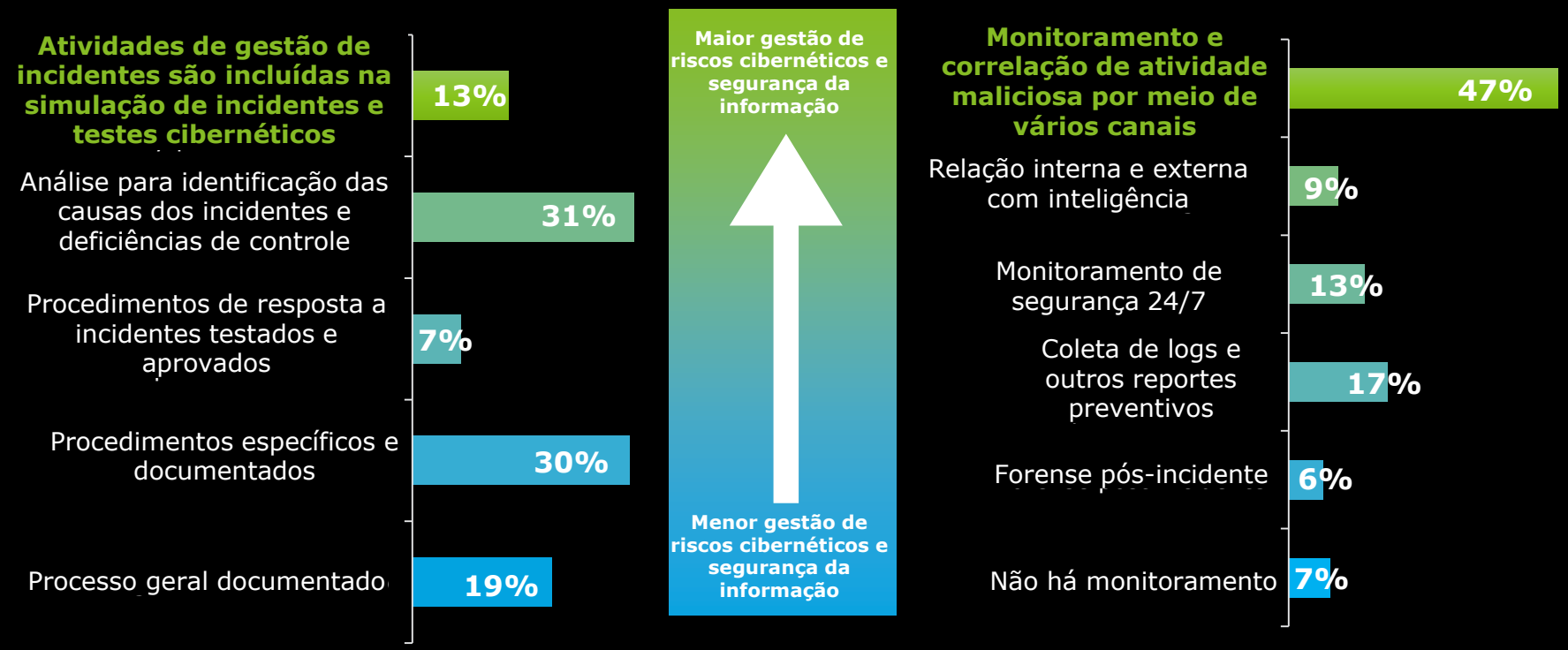


D

As organizações da AL&C devem considerar como altamente provável a ocorrência de um ou vários incidentes de segurança cibernética durante o ano.

Assim como as tendências globais reportadas, muitas das organizações não possuem clareza sobre a quantidade de incidentes sofridos ou impacto causados por eles.

Gestão de incidentes cibernéticos

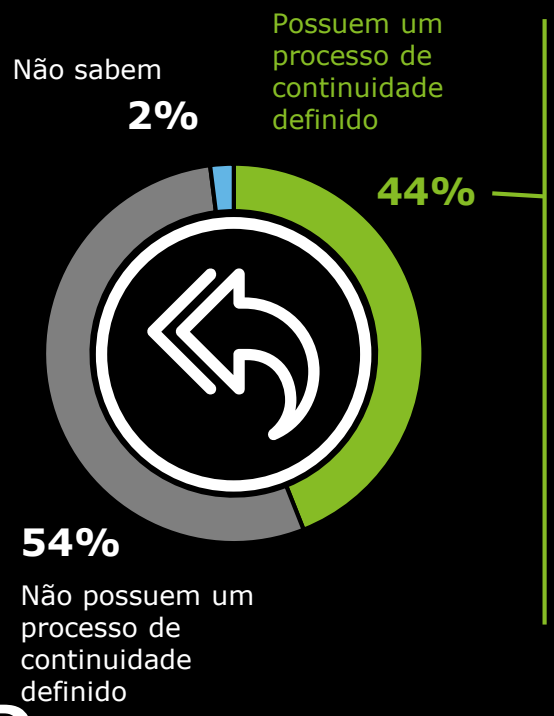


D

Estar preparado para prevenir e responder a incidentes de segurança cibernética deve ser um objetivo estratégico.

Possuir um processo robusto, documentado e testado ainda representa um desafio para as organizações na AL&C.

Cenário cibernético como parte do programa de continuidade de negócios



Os ataques cibernéticos fazem parte do Plano de Continuidade e DRP

35%

Simulações de riscos cibernéticos e de segurança da informação

8%

Testes de bancada

18%

Outros

9%

Bem preparados

Pouca ou nenhuma preparação

D

Mais da metade das organizações na AL&C indicou não contemplar o cenário cibernético dentro de seus programas de continuidade de negócio, e apenas 3% das organizações disseram realizar algum tipo de simulação de um incidente cibernético para validar seu nível de preparação e resposta.

Considerações finais

Considerações finais

1

A evolução dos modelos de negócio, a transformação digital e o contexto das ameaças incentivam as organizações da AL&C a dedicarem mais atenção à gestão de segurança cibernética e a alocarem mais recursos para essa frente.

2

Práticas como o monitoramento de eventos, a inteligência de ameaças e o desenvolvimento de processos de detecção e resposta a incidentes cibernéticos ainda apresentam um nível baixo de maturidade em comparação ao que as próprias organizações manifestam como requeridos.

3

Dado o número de incidentes reportados pelas próprias organizações, é fundamental elevar os esforços para melhorar as capacidades de resposta, incorporando o cenário de eventos cibernéticos dentro dos programas de continuidade e de gestão de crise organizacional.

4

É importante que as organizações verifiquem a eficácia de suas capacidades de proteção, monitoramento e resposta, não apenas para melhorá-las, mas também para assegurar que essas ferramentas funcionarão adequadamente quando necessário.

.

Sobre a Deloitte

Sobre a Deloitte

A Deloitte refere-se a uma firma-membro da Deloitte, uma de suas entidades relacionadas, ou à Deloitte Touche Tohmatsu Limited ("DTTL"). Cada firma-membro da Deloitte é uma entidade legal separada e membro da DTTL. A DTTL não fornece serviços para clientes. Por favor, consulte www.deloitte.com/about para saber mais.

A Deloitte é líder global em auditoria, consultoria empresarial, assessoria financeira, gestão de riscos, consultoria tributária e serviços correlatos. Nossa rede de firmas-membro, presente em mais de 150 países e territórios, atende a quatro de cada cinco organizações listadas pela Fortune Global 500®. Saiba como os 286.200 profissionais da Deloitte impactam positivamente seus clientes em www.deloitte.com.

A prática de **CYBER RISK SERVICES** da Deloitte contribui para que as organizações coloquem em prática suas estratégias de negócio, prestando suporte à gestão dos riscos associados com o desenvolvimento de negócios no setor digital e concorrencial hoje existente.

Com mais de 10.000 especialistas em riscos cibernéticos e segurança da informação em âmbito global, a **Deloitte é líder absoluta em consultoria em riscos cibernéticos e segurança da informação.**

Nosso portfólio de serviços é o mais amplo e completo do mercado, com capacidades locais, regionais e globais colocadas à disposição de nossos clientes.

Na **América Latina e no Caribe temos mais de 600 profissionais e especialistas em riscos cibernéticos e segurança da informação, centros de inteligência cibernética e de prestação de serviços próprios localizados na região**, adaptados às necessidades e riscos locais e regionais.

Para mais informações, visite www.deloitte.com/br/cyber.

Contatos

Andrés Gil
Sócio-líder da prática de Cyber Risk para Américas / líder da prática de Cyber Risk para Argentina & LATCO (Organização de países para América Latina)
angil@deloitte.com

Julio Laurino
Sócio-líder da prática de Cyber Risk Deloitte Brasil
jlaurino@deloitte.com

Nicolás Corrado
Sócio-líder da prática de Cyber Risk Deloitte Chile
nicorrado@deloitte.com

Taron Jackman
Sócio-líder da área de Risk Advisory e da prática de Cyber Risk Caribe
tjackman@deloitte.com

Santiago Gutierrez
Sócio-líder da prática de Cyber Risk Deloitte México
sangutierrez@deloittemx.com

Deloitte.